WHAT IS CLAIMED AS THE INVENTION IS:

1. A method of indicating signature status and trust status of a secure message on a messaging client, the method comprising the steps of:

selecting for processing a secure message stored on the messaging client, the secure message including a digital signature generated by a sender of the secure message;

checking the digital signature;

checking trust status of the sender;

displaying a first indicator of a result of the step of checking the digital signature; and

displaying a second indicator of a result of the step of checking trust status of the sender.

2. The method of claim 1, wherein:

the secure message includes a message body; and

the method further comprises the step of processing the message body.

3. The method of claim 2, wherein:

the step of checking the digital signature comprises determining whether the digital signature is valid or invalid; and

the step of checking trust status comprises determining whether the sender is trusted or untrusted.

4. The method of claim 3, wherein the step of processing is performed only if the digital signature is valid and the sender is trusted.

5. The method of claim 2, wherein the step of processing the secure message comprises displaying the message body on a display screen on the messaging client.

6. The method of claim 3, wherein the first indicator includes a valid signature indication and an invalid signature indication.

7. The method of claim 6, wherein the second indicator includes a trusted indication and an untrusted indication.

8. The method of claim 7, wherein the first and second indicators comprise an icon.

9. The method of claim 7, wherein the first and second indicators comprise text.

10. The method of claim 8, wherein the first and second indicators further comprise text.

11. The method of claim 10, wherein the second indicator comprise a plurality of untrusted indications.

12. The method of claim 11, wherein the plurality of untrusted indications includes an invalid Certificate (Cert) indication, a revoked Cert indication, a missing Cert indication, and

an expired Cert indication.

13. The method of claim 3, wherein:

the digital signature includes a digest and a digest signature; and

the step of checking the digital signature comprises the steps of:

generating a digest of a message body of the secure message;

extracting a digest from the digital signature;

comparing the generated and extracted digests;

checking a digest signature in the digital signature to determine if the digest signature is valid or invalid; and

determining that the digital signature is valid when the generated and extracted digests match and the digest signature is valid.

14. The method of claim 3, wherein:

the secure message also includes a Certificate (Cert) of the sender, the Cert including sender identity information and a public key bound to the sender identity information by a Cert signature generated by an issuer of the Cert; and

the step of checking trust status of the sender comprises the steps of:

checking the Cert signature to determine if the Cert signature is valid or invalid;

if the Cert signature is invalid, then determining that the sender is untrusted; and

if the Cert signature is valid, then

determining whether the issuer of the Cert is a trusted entity;

if the issuer is a trusted entity, then determining that the sender is trusted;

if the issuer is not a trusted entity, then

repeating the steps of checking the Cert signature and determining whether the issuer of the Cert is a trusted entity for each Cert in a Cert chain associated with the Cert of the sender to determine if a valid certification path to a valid root Cert from a trusted entity exists in the chain; and

if a valid certification path to a valid root Cert exists in the chain, then determining that the sender is trusted.

15. The method of claim 14, wherein:

the step of checking trust status of the sender further comprises the steps of:

determining if the Cert of the sender is missing from the secure message and if so, determining that the sender is untrusted;

determining if the Cert of the sender is expired and if so, determining that the sender is untrusted; and

checking a Certificate Revocation List (CRL) to determine if the Cert of the sender has been revoked and if so, determining that the sender is untrusted; and

the step of repeating the steps of checking and determining further comprises repeating the steps of determining if a Cert is expired and checking a CRL.

16. The method of claim 1, wherein the messaging client is operating on a wireless mobile communication device.

17. The method of claim 1, wherein the messaging client is operating on a personal computer system.

18. A system for indicating signature status and trust status of a secure message, comprising:

a messaging client configured to receive secure messages, each of the secure messages including a digital signature generated by a sender of the secure message;

an input configured to receive inputs from a user of the messaging client;

a data processor; and

an output configured to provide outputs to the user,

wherein, when a received secure message is selected for processing by the user via the input, the processor checks the digital signature on the selected secure message, checks the trust status of the sender, and provides separate output indications of the results of the digital signature check and the trust status check on the output.

19. The system of claim 18, wherein the system is selected from the group consisting of: a personal computer system, a networked computer system, a handheld electronic device, a wireless mobile communication device, a cellular telephone, a one-way pager, a two-way pager, a voice communication device, a data communication device, and a dual-mode

communication device.

20. The system of claim 18, wherein the input comprises a keyboard.

21. The system of claim 18, wherein the output comprises a display screen.

22. The system of claim 18, further comprising a memory which stores a plurality of software modules and software applications, including a data communication software module and a secure messaging software application, wherein the processor executes the secure messaging software application to check the digital signature on the selected secure message, to check the trust status of the sender, and to provide the separate output indications.